

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

In the Matter of the Search of

(Briefly describe the property to be searched  
or identify the person by name and address)

N72 W17809 Good Hope Rd. Menomonee Falls, WI, 2008  
Ford F-350, 2013 Jeep Wrangler and 2007 Jeep Patriot,  
as described on Attachment A

Case No. 23-M-535 (SCD)

## WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

To: Any authorized law enforcement officer

An application by a federal law enforcement officer or an attorney for the government requests the search and seizure of the following person or property located in the Eastern District of Wisconsin  
(identify the person or describe the property to be searched and give its location):

See Attachment A

I find that the affidavit(s), or any recorded testimony, establish probable cause to search and seize the person or property described above, and that such search will reveal (identify the person or describe the property to be seized):

See Attachment B

**YOU ARE COMMANDED** to execute this warrant on or before 1-3-24 (not to exceed 14 days)

☒ in the daytime 6:00 a.m. to 10:00 p.m. ☐ at any time in the day or night because good cause has been established.

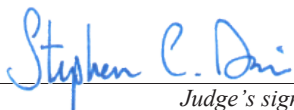
Unless delayed notice is authorized below, you must give a copy of the warrant and a receipt for the property taken to the person from whom, or from whose premises, the property was taken, or leave the copy and receipt at the place where the property was taken.

The officer executing this warrant, or an officer present during the execution of the warrant, must prepare an inventory as required by law and promptly return this warrant and inventory to Honorable Stephen C. Dries  
(United States Magistrate Judge)

☐ Pursuant to 18 U.S.C. § 3103a(b), I find that immediate notification may have an adverse result listed in 18 U.S.C. § 2705 (except for delay of trial), and authorize the officer executing this warrant to delay notice to the person who, or whose property, will be searched or seized (check the appropriate box)

☐ for days (not to exceed 30) ☐ until, the facts justifying, the later specific date of

Date and time issued: 12-20-23. 9:10 am

  
Judge's signature

City and state: Milwaukee, WI

Honorable Stephen C. Dries, U.S. Magistrate Judge  
Printed name and title

<b>Return</b>		
Case No.:	Date and time warrant executed:	Copy of warrant and inventory left with:
Inventory made in the presence of :		
Inventory of the property taken and name(s) of any person(s) seized:		
<b>Certification</b>		
<p>I declare under penalty of perjury that this inventory is correct and was returned along with the original warrant to the designated judge.</p> <div style="display: flex; justify-content: space-between;"> <div style="width: 30%;"> <p>Date: _____</p> </div> <div style="width: 65%;"> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Executing officer's signature</i></p> <p style="text-align: center;">_____</p> <p style="text-align: center;"><i>Printed name and title</i></p> </div> </div>		

### **Attachment A**

#### DESCRIPTION OF LOCATIONS TO BE SEARCHED:

The entire property located at **N72W17809 GOOD HOPE RD, MENOMONEE FALLS, WI**. The location is more particularly described as a one-story single-family residence. This warrant authorizes the search of the SUBJECT PREMISES, any common areas accessible by the occupants of the SUBJECT PREMISES, any storage units or outbuildings associated with the SUBJECT PREMISES, as well as any appurtenances thereto. This warrant further authorizes the search of the following vehicles if located on the SUBJECT PREMISES: 2008 Ford F-350 (WI – XD86426), 2013 Jeep Wrangler (WI – ALY5708), 2007 Jeep Patriot (WI – ADT8690). The exterior of the SUBJECT PREMISES is tan stone siding. A white front door is located on the north side of the building facing Good Hope Road. A chimney is located on the north side of the building to the east of the front door as well as a white-trimmed window to the west of the front door.

Pictures of the residence are provided below:



- Computers and storage media found therein.
- Any person who appears to reside at the SUBJECT PREMISES.

## **Attachment B**

### **Items to be Seized**

1. Cell phones, computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).
4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.
5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of any device by use of the computer or by other

means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).
7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).
8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.
9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic

messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.
11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.
12. Any and all cameras, film, videotapes or other photographic equipment.
13. Any and all visual depictions of minors.
14. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child

pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

16. For any electronic storage device, computer hard drive, electronic device, or other physical object upon which electronic information can be recorded (hereinafter, “electronic storage device”) that is called for by this warrant, or that might contain things otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the electronic storage device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the electronic storage device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the electronic storage device was accessed or used to determine the chronological context of electronic storage device access, use, and events relating to crime under investigation;



- e. evidence indicating the electronic storage device user's location and state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the electronic storage device of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage device;
- h. evidence of the times the electronic storage device was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage device;
- j. documentation and manuals that may be necessary to access the electronic storage device or to conduct a forensic examination of the electronic storage device;
- k. contextual information necessary to understand the evidence described in this attachment.

17. Records and things evidencing the use of the Internet Protocol addresses to communicate with the internet, including:

- a. routers, modems, and network equipment used to connect electronic storage devices to the Internet;
- b. records of Internet Protocol addresses used;
- c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including

any form of electronic storage device or electronic storage; any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form.

During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of residents of the SUBJECT PREMISES to the Touch ID sensor of device(s) or scan for facial recognition, such as an iPhone, Android, or Tablet, found at the premises for the purpose of attempting to unlock the device via fingerprint or facial recognition in order to search the contents as authorized by this warrant. If facial recognition is required, the subject will remain still and look, with eyes open, at the camera for any devices seized in connection with this warrant for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.

Dec 20, 2023

s/ Mariah Kauder

Deputy Clerk, U.S. District Court  
Eastern District of Wisconsin

## UNITED STATES DISTRICT COURT

for the  
Eastern District of Wisconsin

## In the Matter of the Search of

*(Briefly describe the property to be searched  
or identify the person by name and address)*N72 W17809 Good Hope Rd. Menomonee Falls, WI, 2008  
Ford F-350, 2013 Jeep Wrangler and 2007 Jeep Patriot,  
as described on Attachment A

Case No. 23-M-535 (SCD)

## APPLICATION FOR A WARRANT BY TELEPHONE OR OTHER RELIABLE ELECTRONIC MEANS

I, a federal law enforcement officer or an attorney for the government, request a search warrant and state under penalty of perjury that I have reason to believe that on the following person or property *(identify the person or describe the property to be searched and give its location)*:

See Attachment A

located in the Eastern District of Wisconsin, there is now concealed *(identify the person or describe the property to be seized)*:

See Attachment B

The basis for the search under Fed. R. Crim. P. 41(c) is *(check one or more)*:

- ☒ evidence of a crime;
- ☒ contraband, fruits of crime, or other items illegally possessed;
- ☒ property designed for use, intended for use, or used in committing a crime;
- ☐ a person to be arrested or a person who is unlawfully restrained.

The search is related to a violation of:

Code Section	Offense Description
18 U.S.C. § 2252(a)(2);	Distribution of child pornography;
18 U.S.C. § 2252(a)(4)(B)	Possession of child pornography

The application is based on these facts:

See attached affidavit

- ☒ Continued on the attached sheet.
- ☐ Delayed notice of \_\_\_\_\_ days *(give exact ending date if more than 30 days)* \_\_\_\_\_ is requested under 18 U.S.C. § 3103a, the basis of which is set forth on the attached sheet.

Applicant's signature

Daniel Gartland, Special Agent - FBI

Printed name and title

Attested to by the applicant in accordance with the requirements of Fed. R. Crim. P. 4.1 by  
telephone \_\_\_\_\_ *(specify reliable electronic means)*.

Date: 12-20-23

Judge's signature

City and state: Milwaukee, WI

Honorable Stephen C. Dries, U.S. Magistrate Judge

Printed name and title

## **AFFIDAVIT IN SUPPORT OF AN APPLICATION FOR A SEARCH WARRANT**

I, Daniel Gartland, being first duly sworn, depose and state as follows:

### **INTRODUCTION AND AGENT BACKGROUND**

1. I am a Special Agent (SA) with the Federal Bureau of Investigation (FBI) and have been so employed since May 2018. As such, I am a "federal law enforcement officer" within the meaning of Federal Rule of Criminal Procedure 41(a)(2)(C), that is, a government agent engaged in enforcing the criminal laws and duly authorized by the Attorney General to request search and arrest warrants. I am currently assigned to the FBI Milwaukee Division and am a member of the Milwaukee Child Exploitation and Human Trafficking Task Force. I am authorized to investigate violent crimes against children, to include the possession, production, and distribution of child sexual abuse material (commonly known as "CSAM"). While employed by the FBI, I have investigated federal criminal violations related to child exploitation, and child pornography. I have received training to investigate child pornography and child exploitation crimes and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256) in different forms of media including computer media. As a result of my training, experience, and discussions with other law enforcement officers assigned to investigate child pornography and child exploitation, I am familiar with methods by which electronic devices are used as the means for receiving, transmitting, possessing, and distributing images and videos depicting minors engaged in sexually explicit conduct. I have also received training and gained experience in interview and interrogation techniques with enhanced training specific to cybercrimes, social media search warrants, residential search warrants, interviews and interrogations of subjects of criminal investigations, as well as electronic device identification and forensic review.

2. The facts contained in this affidavit are known to me through my personal knowledge, training, and experience, and through information provided to me by other law enforcement officers, who have provided information to me during the course of their official duties and whom I consider truthful and reliable.

3. Based upon the information described below, I submit that probable cause exists to believe that the subject(s) residing at N72W17809 GOOD HOPE RD, MENOMONEE FALLS, WI (SUBJECT PREMISES) has committed the crimes of distribution of child pornography in violation of Title 18, United States Code, Section 2252(a)(2), and possession of child pornography in violation of Title 18, United States Code, Section 2252(a)(4)(B). I further submit that evidence relating to this crime, more particularly described in Attachment B, can be found in the SUBJECT PREMISES, more particularly described in Attachment A.

4. This affidavit is intended to show only that there is sufficient probable cause for the requested warrant and does not set forth all of my knowledge about this matter.

#### DEFINITIONS

5. The following definitions apply to the Affidavit and Attachment B to this Affidavit:

a. “Child Pornography” is defined in 18 U.S.C. § 2256(8) as any visual depiction of sexually explicit conduct where (a) the production of the visual depiction involved the use of a minor engaged in sexually explicit conduct, (b) the visual depiction is a digital image, computer image, or computer-generated image that is, or is indistinguishable from, that of a minor engaged in sexually explicit conduct, or (c) the visual depiction has been created, adapted, or modified to appear that an identifiable minor is engaged in sexually explicit conduct.

b. “Child erotica” means materials or items that are sexually arousing to persons having a sexual interest in minors but that are not necessarily obscene or do not necessarily depict minors in sexually explicit poses or positions.

c. “Computer” refers to “an electronic, magnetic, optical, electrochemical, or other high speed data processing device performing logical or storage functions, and includes any data storage facility or communications facility directly related to or operating in conjunction with such device” and includes smartphones, and mobile phones and devices. See 18 U.S.C. § 1030(e)(1).

d. “Computer hardware” consists of all equipment that can receive, capture, collect, analyze, create, display, convert, store, conceal, or transmit electronic, magnetic, or similar computer impulses or data. Computer hardware includes any data-processing devices (including central processing units, internal and peripheral storage devices such as fixed disks, external hard drives, floppy disk drives and diskettes, and other memory storage devices); peripheral input/output devices (including keyboards, printers, video display monitors, and related communications devices such as cables and connections); as well as any devices, mechanisms, or parts that can be used to restrict access to computer hardware (including physical keys and locks).

e. “Chat,” as used herein, refers to any kind of text communication over the Internet that is transmitted in real-time from sender to receiver. Chat messages are generally short in order to enable other participants to respond quickly and in a format that resembles an oral

conversation. This feature distinguishes chatting from other text-based online communications such as Internet forums and email.

f. The “Internet” is a global network of computers and other electronic devices that communicate with each other. Due to the structure of the Internet, connections between devices on the Internet often cross state and international borders, even when the devices communicating with each other are in the same state.

g. An “Internet Protocol address” (IP address) is a unique numeric address used by internet-enabled electronic storage devices to access the Internet. An IP address is a series of four numbers, each in the range 0-255, separated by periods (e.g., 121.56.97.178). Every electronic storage device attached to the Internet must be assigned an IP address so that Internet traffic sent from and directed to that electronic storage device may be directed properly from its source to its destination. Most Internet service providers control a range of IP addresses. Some computers have static that is, long-term IP addresses, while other computers have dynamic that is, frequently changed IP addresses.

h. “Internet Service Providers” (“ISPs”) are commercial organizations that are in business to provide individuals and businesses access to the Internet. ISPs provide a range of functions for their customers including access to the Internet, web hosting, e-mail, remote storage, and co-location of computers and other communications equipment.

i. “Minor” means any person under the age of eighteen years. See 18 U.S.C. § 2256(1).

j. The terms “records,” “documents,” and “materials” include all information recorded in any form, visual or aural, and by any means, whether in handmade form (including writings and drawings), photographic form (including prints, negatives, videotapes, motion pictures, and photocopies), mechanical form (including printing and typing) or electrical, electronic or magnetic form (including tape recordings, compact discs, electronic or magnetic storage devices such as hard disks, CD-ROMs, digital video disks (DVDs), Personal Digital Assistants (PDAs), Multi Media Cards (MMCs), memory sticks, smart cards, or electronic notebooks, as well as digital data files and printouts or readouts from any magnetic, electrical or electronic storage device).

k. “Sexually explicit conduct” means actual or simulated (a) sexual intercourse, including genital-genital, oral-genital, or oral-anal, whether between persons of the same or opposite sex; (b) bestiality; (c) masturbation; (d) sadistic or masochistic abuse; or (e) lascivious exhibition of the genitals or pubic area of any person. See 18 U.S.C. § 2256(2).

l. “Visual depictions” include undeveloped film and videotape, and data stored on a computer disk or by electronic means, which is capable of conversion into a visual image. See 18 U.S.C. § 2256(5).

m. “Website” consists of text pages of information and associated graphic images. The textual information is stored in a specific format known as Hyper-Text Mark-up Language (HTML) and is transmitted from the web servers to various web clients via Hyper-Text Transport Protocol.



## **ELECTRONIC STORAGE DEVICES AND FORENSIC ANALYSIS**

6. I am aware through training, experience, and consulting with other law enforcement agents/analysts with specialized knowledge and training in computers, networks, and Internet communications that to properly retrieve and analyze electronically stored (computer) data, and to ensure accuracy and completeness of such data and to prevent loss of the data either from accidental or programmed destruction, it is necessary to conduct a forensic examination of the electronic storage devices. To ensure such accuracy and completeness, it may also be necessary to analyze not only the electronic storage devices, but also peripheral devices which may be interdependent, the software to operate them, and related instruction manuals containing directions concerning operation of the device computer and software. As described above and in Attachment B, this application seeks permission to search and seize records that might be found on the proposed search location, in whatever form they are found. One form in which the records might be found is stored on a computer's hard drive, other storage media, within a hand-held electronic device such as a cellular telephone or a tablet device (e.g., an iPad device). Some of this electronic information, as explained below, might take a form that becomes meaningful only upon forensic analysis.

7. Based on my knowledge, training, and experience, I know that computer and other electronic device hardware, peripheral devices, software, documentation, and passwords may be important to a criminal investigation in three distinct and important respects.

- a. The objects themselves may be instrumentalities used to commit the crime;
- b. the objects may have been used to collect and store information about crimes (in the form of electronic data); and

c. the objects may be contraband or fruits of the crime.

8. I submit that if a computer or other electronic storage device is found on the premises, there is probable cause to believe those records will be stored in that electronic storage device, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that electronic storage device files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person deletes a file on an electronic storage device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data. It follows that deleted files, or remnants of deleted files, may reside in free space or slack space that is, in space on the storage medium that is not currently being used by an active file for long periods of time before they are overwritten. In addition, if the electronic storage device uses an operating system (in the case, for example, of a computer, cellular telephone, or tablet device) the device may also contain a record of deleted data in a swap or recovery file.

b. Wholly apart from user-generated files, electronic storage device storage media in particular, computers' internal hard drives, contain electronic evidence of how the device was used, what it has been used for, and who has used it. This evidence can take the form of operating system configurations, artifacts from operating system or application operation, and file system data structures. Electronic storage device users typically do not erase or delete this evidence

because special software is typically required for that task. However, it is technically possible to delete this information.

c. Files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or cache. The browser often maintains a fixed amount of hard drive space devoted to these files, and the files are only overwritten as they are replaced with more recently viewed Internet pages or if a user takes steps to delete them.

9. As further described in Attachment B, this application seeks permission to locate not only electronic storage device files that might serve as direct evidence of the crimes described on the warrant, but also for evidence that establishes how electronic storage devices were used, the purpose of their use, who used them, and when.

10. Although some of the records called for by this warrant might be found in the form of user-generated documents (such as word processor, picture, and movie files), electronic storage device storage media can contain other forms of electronic evidence as described below:

a. Data on the storage medium not currently associated with any file can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the electronic storage device was in use. Electronic storage device file systems can record information about the dates files were created and the sequence in which they were created.

b. As explained herein, information stored within an electronic storage device and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within an electronic storage device (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the electronic storage device. This “user attribution” evidence is analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the electronic storage device was remotely accessed, thus inculcating or exculpating the electronic storage device owner. Further, electronic storage device activity can indicate how and when the electronic storage device was accessed or used. For example, as described herein, computers typically contain information that logs computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within an electronic storage device may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer or cellular telephone may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also

contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera). The geographic and timeline information described herein may either inculcate or exculpate the electronic storage device user. Last, information stored within an electronic storage device may provide relevant insight into the device user's state of mind as it relates to the offense under investigation. For example, information within the electronic storage device may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the electronic storage device or password protecting/encrypting such evidence in an effort to conceal it from law enforcement).

c. The process of identifying the exact files, blocks, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. Whether data stored on an electronic storage device is relevant to the investigation may depend on other information stored on the electronic storage device and the application of knowledge about how an electronic storage device works. Therefore, contextual information necessary to understand the evidence described in Attachment B also falls within the scope of the warrant.

d. Further, in finding evidence of how an electronic storage device was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, I know from training and experience that it is possible that malicious software can be installed on a computer, often without the computer

user's knowledge, that can allow the computer to be used by others, sometimes without the knowledge of the computer owner.

11. Based upon my knowledge, training and experience, and after having consulted with FBI computer forensic personnel, I know that a thorough search for information stored in storage media often requires agents to seize most or all storage media to be searched later in a controlled environment. This is often necessary to ensure the accuracy and completeness of data recorded on the storage media, and to prevent the loss of the data either from accidental or intentional destruction. Additionally, to properly examine the storage media in a controlled environment, it is often necessary that some electronic storage device equipment, peripherals, instructions, and software be seized and examined in the controlled environment. This is true because of the following:

a. The nature of evidence. As noted above, not all evidence takes the form of documents and files that can be easily viewed on site. Analyzing evidence of how an electronic storage device has been used, what it has been used for, and who has used it requires considerable time, and taking that much time on premises could be unreasonable.

b. The volume of evidence. Storage media can store the equivalent of millions of pages of information. Additionally, a suspect may try to conceal criminal evidence; he or she might store it in random order with deceptive file names. This may require searching authorities to peruse all the stored data to determine which particular files are evidence or instrumentalities of crime. This sorting process can take weeks or months, depending on the volume of data stored, and it would be impractical and invasive to attempt this kind of data search on-site.

c. Technical requirements. Electronic storage devices can be configured in several different ways, featuring a variety of different operating systems, application software, and configurations. Therefore, searching them sometimes requires tools or knowledge that might not be present on the search site. The vast array of electronic storage device hardware and software available makes it difficult to know before a search what tools or knowledge will be required to analyze the system and its data on-site. However, taking the storage media off-site and reviewing it in a controlled environment will allow its examination with the proper tools and knowledge.

d. Variety of forms of electronic media. Records sought under this warrant could be stored in a variety of storage media formats that may require off-site reviewing with specialized forensic tools.

12. In light of these concerns, I hereby request the Court's permission to seize the electronic storage devices, associated storage media, and associated peripherals that are believed to contain some or all of the evidence described in the warrant, and to conduct an off-site search of the hardware for the evidence described, if, upon arriving at the scene, the agents executing the search conclude that it would be impractical to search the hardware, media, or peripherals on-site for this evidence.

13. I know that when an individual uses a computer to commit crimes involving child pornography, the individuals' computer and/or electronic devices will generally serve both as an instrumentality for committing the crime, and also as a storage medium for evidence of the crime. The electronic storage device is an instrumentality of the crime because it is used as a means of committing the criminal offense. From my training and experience, I believe that an electronic storage device used to commit a crime of this type may contain data that is evidence of how the

electronic storage device was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

### **BIOMETRIC ACCESS TO DEVICES**

14. I know from my training and experience, as well as from information found in publicly available materials published by device manufacturers, that many electronic devices, particularly newer mobile devices and laptops, offer their users the ability to unlock the device through biometric features in lieu of a numeric or alphanumeric passcode or password. These biometric features include fingerprint scanners, facial recognition features and iris recognition features. Some devices offer a combination of these biometric features, and the user of such devices can select which features they would like to utilize.

15. If a device is equipped with a fingerprint scanner, a user may enable the ability to unlock the device through his or her fingerprints. For example, Apple offers a feature called “Touch ID,” which allows a user to register up to five fingerprints that can unlock a device. Once a fingerprint is registered, a user can unlock the device by pressing the relevant finger to the device’s Touch ID sensor, which is found in the round button (often referred to as the “home” button) located at the bottom center of the front of the device. The fingerprint sensors found on devices produced by other manufacturers have different names but operate similarly to Touch ID.

16. If a device is equipped with a facial-recognition feature, a user may enable the ability to unlock the device through his or her face. For example, this feature is available on certain Android devices and is called “Trusted Face.” During the Trusted Face registration process, the user holds the device in front of his or her face. The device’s front-facing camera then analyzes



and records data based on the user's facial characteristics. The device can then be unlocked if the front-facing camera detects a face with characteristics that match those of the registered face. Facial recognition features found on devices produced by other manufacturers have different names but operate similarly to Trusted Face.

17. If a device is equipped with an iris-recognition feature, a user may enable the ability to unlock the device with his or her irises. For example, on certain Microsoft devices, this feature is called "Windows Hello." During the Windows Hello registration, a user registers his or her irises by holding the device in front of his or her face. The device then directs an infrared light toward the user's face and activates an infrared-sensitive camera to record data based on patterns within the user's irises. The device can then be unlocked if the infrared-sensitive camera detects the registered irises. Iris-recognition features found on devices produced by other manufacturers have different names but operate similarly to Windows Hello.

18. In my training and experience, users of electronic devices often enable the aforementioned biometric features because they are considered to be a more convenient way to unlock a device than by entering a numeric or alphanumeric passcode or password. Moreover, in some instances, biometric features are considered to be a more secure way to protect a device's contents. This is particularly true when the users of a device are engaged in criminal activities and thus have a heightened concern about securing the contents of a device.

19. As discussed in this Affidavit, I have reason to believe that one or more digital devices will be found during the search. The passcode or password that would unlock the devices subject to search under this warrant currently is not known to law enforcement. Thus, law enforcement personnel may not otherwise be able to access the data contained within the devices,

making the use of biometric features necessary to the execution of the search authorized by this warrant.

20. I also know from my training and experience, as well as from information found in publicly available materials including those published by device manufacturers, that biometric features will not unlock a device in some circumstances even if such features are enabled. This can occur when a device has been restarted, inactive, or has not been unlocked for a certain period of time. For example, Apple devices cannot be unlocked using Touch ID when: (1) more than 48 hours has elapsed since the device was last unlocked; or (2) when the device has not been unlocked using a fingerprint for 8 hours and the passcode or password has not been entered in the last 6 days. Similarly, certain Android devices cannot be unlocked with Trusted Face if the device has remained inactive for four hours. Biometric features from other brands carry similar restrictions. Thus, in the event law enforcement personnel encounter a locked device equipped with biometric features, the opportunity to unlock the device through a biometric feature may exist for only a short time.

21. Due to the foregoing, if law enforcement personnel encounter any devices that are subject to seizure pursuant to this warrant and may be unlocked using one of the aforementioned biometric features, I request authority for law enforcement personnel to: (1) press or swipe the fingers (including thumbs) of the residents of the SUBJECT PREMISES to the fingerprint scanner of the devices found at the SUBJECT PREMISES, in the SUBJECT VEHICLE, or on residents of the SUBJECT PREMISES' person(s); (2) hold the devices found at the SUBJECT PREMISES, in the SUBJECT VEHICLE, or on the person of residents of the SUBJECT PREMISES in front of residents of the SUBJECT PREMISES' face to activate the facial recognition feature; and/or (3)

hold the devices found at the SUBJECT PREMISES, in the SUBJECT VEHICLE, or on the person of residents of the SUBJECT PREMISES in front of residents of the SUBJECT PREMISES' face and activate the iris recognition feature, for the purpose of attempting to unlock the devices in order to search the contents as authorized by this warrant.

### **BACKGROUND ON PEER TO PEER FILE SHARING**

22. A significant aspect of the internet, as it relates to this investigation, is peer to peer (P2P) file sharing. P2P file sharing is a method of communication available to internet users through the use of widely available software. This investigation focuses on the P2P network called BitTorrent. There are several different software applications that can be used to access these different P2P networks and these applications operate in essentially the same manner. Computers linked together through the internet using this software form a network that allows for the sharing of digital files between users on the network.

23. These P2P networks are commonly referred to as decentralized networks because each user of the network is able to distribute information and queries directly through other users of the network, rather than relying on a central server to act as an indexing agent, where all of the information is first deposited before it is distributed.

24. To access the P2P networks user must first obtain the required P2P software, this software can be downloaded for free from the internet. In general, P2P software allows the user to set up files on a computer to be shared with others running compatible P2P software. When the P2P software is installed on a computer, the user is directed to specify a "shared" folder. All files placed in that user's "shared" folder are available to be shared with and download by any other user connected to the P2P network. Therefore, a user needs simply to move a file from one folder

to another to stop the distribution across the internet. Further, once a file or files are placed in a shared folder the distribution of that file(s) is dependent only on the machine being turned on and connected to the internet.

25. The BitTorrent network is a very popular and publicly available P2P filesharing network. Most computers that are part of this network are referred to as "peers" or "clients." A peer/client can simultaneously provide files to some peers/clients while downloading files from other peers/clients. The BitTorrent network can be accessed by peer/client computers via many different BitTorrent network client (software) programs, including uTorrent, Vuze, Deluge, qBittorrent, and others. These are publicly available and typically free P2P client software programs that can be downloaded from the internet.

26. BitTorrent sets up its searches by keywords typically on torrent websites. The results of a keyword search are displayed to the user. The website does not contain the files being shared, only the file referred to as a "torrent." A torrent file defines the files being shared and contains file names, file sizes, file paths, the total number of pieces, the size of each piece, the SHA-1 hash value of each piece, and the torrent type (public or private). The torrent file does not contain the desired content; it simply defines what is available. A user may then select a torrent file(s) from the search results for download. For example, a person interested in obtaining child pornography images/videos could open the BitTorrent website on his/her computer and conduct a keyword search for files using a term such as "preteen sex." The results of the search are returned to the user's computer and displayed on the torrent site. The user then selects a torrent from the results displayed which contain the file(s) the user wants to download. Once the torrent file is downloaded, the user's previously installed BitTorrent client program utilizes the torrent file to

obtain the desired content on the network. The file is downloaded directly from the computer or computers sharing the file. The users can receive pieces of the selected file from numerous sources at once, or it can be from a single source. Once received, the pieces are then reassembled into the entire selected file. The downloaded file is stored in a folder previously designated by the user and/or the client program on the user's computer or designated external storage media or location on the user's computer. The downloaded file will remain until moved or deleted.

27. One of the advantages of P2P file sharing is that multiple files may be downloaded at the same time. In addition, a user may download parts of one file from more than one source computer at a time. For example, a BitTorrent user downloading a movie file may actually receive parts of the movie from multiple computers. The advantage of this is that it speeds up the time it takes to download the file. It is also possible to download the file or files from only one computer.

28. The BitTorrent Network bases its file shares on the Secure Hash Algorithm (SHA1). This mathematical algorithm allows for the digital fingerprinting of data. Once you check a file or files with a SHA1 hashing utility capable of generating this SHA1 value (the fingerprint), that will be a fixed-length unique identifier for that file. The SHA1 is secure because it is computationally infeasible for two files with different content to have the same SHA1 hash value.

29. A P2P file transfer is assisted by reference to an Internet Protocol (IP) address. This address, expressed as four numbers separated by decimal points, is unique to a particular computer during an online session. The IP address provides a unique location making it possible for data to be transferred between computers. Most P2P software does not display the IP address of the person sharing the file to the user. Third party software is available to identify the IP address of the P2P computer sharing a particular file.

30. IP addresses can be dynamic, meaning that the Internet Service Provider (ISP) can assign a different unique number to a computer when it accesses the internet. IP addresses might also be static, if an ISP assigns a user's computer a particular IP address which is used each time the computer accesses the internet.

**SPECIFICS OF SEARCH AND SEIZURE OF COMPUTER SYSTEMS.**

31. As described above and in Attachment B, this application seeks permission to search for records that might be found on the SUBJECT PREMISES, in whatever form they are found. One form in which the records might be found is data stored on a computer's hard drive or other storage media. Thus, the warrant applied for would authorize the seizure of electronic storage media or, potentially, the copying of electronically stored information, all under Rule 41(e)(2)(B).

32. I submit that if a computer or storage medium is found on the SUBJECT PREMISES, there is probable cause to believe those records will be stored on that computer or storage medium, for at least the following reasons:

a. Based on my knowledge, training, and experience, I know that computer files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a computer, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

b. Therefore, deleted files, or remnants of deleted files, may reside in free space or slack space—that is, in space on the storage medium that is not currently being used by an active file—for long periods of time before they are overwritten. In addition, a computer’s operating system may also keep a record of deleted data in a “swap” or “recovery” file.

c. Wholly apart from user-generated files, computer storage media—in particular, computers’ internal hard drives—contain electronic evidence of how a computer has been used, what it has been used for, and who has used it. To give a few examples, this forensic evidence can take the form of operating system configurations, artifacts from operating system or application operation, file system data structures, and virtual memory “swap” or paging files. Computer users typically do not erase or delete this evidence, because special software is typically required for that task. However, it is technically possible to delete this information.

d. Similarly, files that have been viewed via the Internet are sometimes automatically downloaded into a temporary Internet directory or “cache.”

33. As further described in Attachment B, this application seeks permission to locate not only computer files that might serve as direct evidence of the crimes described on the warrant, but also for forensic electronic evidence that establishes how computers were used, the purpose of their use, who used them, and when. There is probable cause to believe that this forensic electronic evidence will be on any storage medium in the PREMISES because:

a. Data on the storage medium can provide evidence of a file that was once on the storage medium but has since been deleted or edited, or of a deleted portion of a file (such as a paragraph that has been deleted from a word processing file). Virtual memory paging systems can leave traces of information on the storage medium that show what tasks and processes were recently active. Web browsers, e-mail programs, and chat programs store configuration information on the storage medium that can reveal information such as online nicknames and passwords. Operating systems can record additional information, such as the attachment of peripherals, the attachment of USB flash storage devices or other external storage media, and the times the computer was in use. Computer file systems can record information about the dates files were created and the sequence in which they were created, although this information can later be falsified.

b. As explained herein, information stored within a computer and other electronic storage media may provide crucial evidence of the “who, what, why, when, where, and how” of the criminal conduct under investigation, thus enabling the United States to establish and prove each element or alternatively, to exclude the innocent from further suspicion. In my training and experience, information stored within a computer or storage media (e.g., registry information, communications, images and movies, transactional information, records of session times and durations, internet history, and anti-virus, spyware, and malware detection programs) can indicate who has used or controlled the computer or storage media. This “user attribution” evidence is



analogous to the search for “indicia of occupancy” while executing a search warrant at a residence. The existence or absence of anti-virus, spyware, and malware detection programs may indicate whether the computer was remotely accessed, thus inculcating or exculpating the computer owner. Further, computer and storage media activity can indicate how and when the computer or storage media was accessed or used. For example, as described herein, computers typically contain information that log computer user account session times and durations, computer activity associated with user accounts, electronic storage media that connected with the computer, and the IP addresses through which the computer accessed networks and the internet. Such information allows investigators to understand the chronological context of computer or electronic storage media access, use, and events relating to the crime under investigation. Additionally, some information stored within a computer or electronic storage media may provide crucial evidence relating to the physical location of other evidence and the suspect. For example, images stored on a computer may both show a particular location and have geolocation information incorporated into its file data. Such file data typically also contains information indicating when the file or image was created. The existence of such image files, along with external device connection logs, may also indicate the presence of additional electronic storage media (e.g., a digital camera or cellular phone with an incorporated camera). The geographic and timeline information described herein may either inculcate or exculpate the computer user. Last, information stored within a computer may provide relevant insight into the

computer user's state of mind as it relates to the offense under investigation. For example, information within the computer may indicate the owner's motive and intent to commit a crime (e.g., internet searches indicating criminal planning), or consciousness of guilt (e.g., running a "wiping" program to destroy evidence on the computer or password protecting/encrypting such evidence to conceal it from law enforcement).

c. A person with appropriate familiarity with how a computer works can, after examining this forensic evidence in its proper context, draw conclusions about how computers were used, the purpose of their use, who used them, and when.

d. The process of identifying the exact files, pieces, registry entries, logs, or other forms of forensic evidence on a storage medium that are necessary to draw an accurate conclusion is a dynamic process. While it is possible to specify in advance the records to be sought, computer evidence is not always data that can be merely reviewed by a review team and passed along to investigators. Whether data stored on a computer is evidence may depend on other information stored on the computer and the application of knowledge about how a computer behaves. Therefore, contextual information necessary to understand other evidence also falls within the scope of the warrant.

e. Further, in finding evidence of how a computer was used, the purpose of its use, who used it, and when, sometimes it is necessary to establish that a particular thing is not present on a storage medium. For example, the presence or absence of

counter-forensic programs or anti-virus programs (and associated data) may be relevant to establishing the user's intent.

f. I know that when an individual uses a computer to obtain or access child pornography, the individual's computer will generally serve both as an instrumentality for committing the crime, and as a storage medium for evidence of the crime. The computer is an instrumentality of the crime because it is used as a means of committing the criminal offense. The computer is also likely to be a storage medium for evidence of crime. From my training and experience, I believe that a computer used to commit a crime of this type may contain data that is evidence of how the computer was used; data that was sent or received; notes as to how the criminal conduct was achieved; records of Internet discussions about the crime; and other records that indicate the nature of the offense.

34. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage. I also know that during the search of the premises it is not always possible to

search computer equipment and storage devices for data for several reasons, including the following:

a. Searching computer systems is a highly technical process which requires specific expertise and specialized equipment. There are so many types of computer hardware and software in use today that it is impossible to bring to the search site all the technical manuals and specialized equipment necessary to conduct a thorough search. In addition, it may also be necessary to consult with computer personnel who have specific expertise in the type of computer, software website, or operating system that is being searched;

b. Searching computer systems requires the use of precise, scientific procedures which are designed to maintain the integrity of the evidence and to recover “hidden,” erased, compressed, encrypted, or password-protected data. Computer hardware and storage devices may contain “booby traps” that destroy or alter data if certain procedures are not scrupulously followed. Since computer data is particularly vulnerable to inadvertent or intentional modification or destruction, a controlled environment, such as a law enforcement laboratory, is essential to conducting a complete and accurate analysis of the equipment and storage devices from which the data will be extracted;

c. The volume of data stored on many computer systems and storage devices will typically be so large that it will be highly impractical to search for data during the execution of the physical search of the premises; and

d. Computer users can attempt to conceal data within computer equipment and storage devices through several methods, including the use of innocuous or misleading filenames and extensions. For example, files with the extension “.jpg” often are image files; however, a user can easily change the extension to “.txt” to conceal the image and make it appear that the file contains text. Computer users can also attempt to conceal data by using encryption, which means that a password or device, such as a “dongle” or “keycard,” is necessary to decrypt the data into readable form. In addition, computer users can conceal data within another seemingly unrelated and innocuous file in a process called “steganography.” For example, by using steganography a computer user can conceal text in an image file which cannot be viewed when the image file is opened. Therefore, a substantial amount of time is necessary to extract and sort through data that is concealed or encrypted to determine whether it is contraband, evidence, fruits, or instrumentalities of a crime.

35. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called “wireless routers,” which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be “secured” (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or “unsecured” (in that an individual

may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime – including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

36. Based on the foregoing, and consistent with Rule 41(e)(2)(B), the warrant I am applying for would permit seizing, imaging, or otherwise copying storage media that reasonably appear to contain some or all the evidence described in the warrant and would authorize a later review of the media or information consistent with the warrant. The later review may require techniques, including but not limited to computer-assisted scans of the entire medium, that might expose many parts of a hard drive to human inspection in order to determine whether it is evidence described by the warrant.

#### **BACKGROUND OF THE INVESTIGATION AND PROBABLE CAUSE**

37. On or about June 16, 2023, Special Agent Sarah Dettmering was conducting an online investigation on the BitTorrent network for offenders sharing CSAM. An investigation was initiated for a device being operated with the IP Address 72.135.253.219 because it was associated with a shared torrent which contained at least one file consistent with the definition of CSAM.

38. Using a computer running investigative BitTorrent software, a direct connection was made to the device at IP Address 72.135.253.219 and a download was successfully completed of files with the names 000040.jpg and 0000364.jpg. The device at IP Address 72.135.253.219 was the sole candidate for this download, and as such, this file was downloaded directly from this IP address. This files are described as follows:

- a. A collection of 20 images that appear to be from the same video. The images are displayed in a grid and each contain a separate timestamp. The images show a prepubescent girl, approximately three to five years old completely nude. In one image, the girl is facing the camera with her legs spread to expose her vagina. An adult hand is touching the girl's vagina. In five of the images, the girl is performing oral sex on what appears to be an adult male.
- b. A collection of 20 images that appear to be from the same video. The images are displayed in a grid and each contain a separate timestamp. The images show a prepubescent girl, approximately four to six years old completely nude. Twelve of the images show the girl lying on her back with her legs spread to expose her vagina with what appears to be an adult inserting his penis into her anus.

39. The most recent direct connection and download from the device at IP Address 72.135.253.219 was made on 09/11/2023.

40. On or about June 20, 2023 an administrative subpoena was served on Charter Communications Inc. (Charter), by an Operational Support Technician for the FBI, for the IP Address 72.135.253.219 on the dates of the above described downloads. On or about June 22, 2023 Charter provided a response to the administrative subpoena, which contained the following information:

- a. Subscriber Name: Ruben Vega
- b. Address: N72W17809 GOOD HOPE RD, MENOMONEE FALLS, WI [SUBJECT PREMISES]
- c. Lease Start Date: 05/09/2023 at 6:09 AM

41. On or about September 20, 2023 an administrative subpoena was again served on Charter Communications Inc. (Charter), by an Operational Support Technician for the FBI, for the IP Address 72.135.253.219 on the dates of the above described downloads. On or about September 25, 2023 Charter provided a response to the administrative subpoena, which contained the following information:

- a. Subscriber Name: Ruben Vega
- b. Address: N72W17809 GOOD HOPE RD, MENOMONEE FALLS, WI [SUBJECT PREMISES]
- c. Lease Start Date: 12/19/2010

42. Since approximately July 26, 2023, surveillance was conducted at the SUBJECT PREMISES. The proximity of the SUBJECT PREMISES to the nearest public road created difficulty in determining the individuals who resided at the SUBJECT PREMISES, however, this affiant observed the same vehicles entering and exiting the driveway and yard of the SUBJECT PREMISES for the duration of the surveillance. The vehicles included a blue Toyota Rav4, a white Ford F350, a black Jeep Wrangler, a black Ford Explorer, and a blue Jeep Patriot, among others.

43. Law enforcement records show that a Ruben Vega-Rojo (DOB XX/XX/1974) resides at the SUBJECT PREMISES. Among the vehicles registered to VEGA-ROJO are a white Ford F350, a black Jeep Wrangler, and a blue Jeep Patriot, all of which were consistently observed during surveillance.

44. On December 6, 2023, Special Agents and Task Force Officers with the Federal Bureau of Investigation attempted to serve a residential search warrant on the premises. A change in the pattern of life by the occupants of the residence on the planned date of execution made the



operational plan to secure the residence not feasible. The warrant could not be executed prior to the expiration on December 15, 2023. The warrant was returned unexecuted on December 18, 2023.

45. Based upon the above, particularly the fact that the IP Address that made the files available was registered to the SUBJECT PREMISES at the time of the uploads, it appears as though the uploads were made from someone at the SUBJECT PREMISES. As such, I believe there is probable cause to believe that evidence of the BitTorrent distributions will still be at the SUBJECT PREMISES, in the SUBJECT VEHICLES, or on the person of the residents of the SUBJECT PREMISES.

**BACKGROUND ON CHILD PORNOGRAPHY, COMPUTERS, AND THE  
INTERNET**

46. I have had both training and experience in the investigation of computer-related crimes. Based on my training, experience, and knowledge, I know the following:

a. Computers, cellular telephones, and other electronic storage devices (collectively electronic storage devices) have dramatically changed the way in which individuals interested in child pornography interact with each other. Electronic storage devices basically serve four functions in connection with child pornography: production, communication, distribution, and storage.

b. Child pornographers can now transfer printed photographs into a computer-readable format with a device known as a scanner. Furthermore, with the advent of digital cameras, when the photograph is taken it is saved as a digital file that can be directly transferred to a device by simply connecting the camera to the electronic storage device. In the last ten years, the resolution of pictures taken by digital cameras has increased dramatically, meaning the photos

taken with digital cameras have become sharper and crisper. Photos taken on a digital camera are stored on a removable memory card in the camera. These memory cards often store terabytes of data, which provides enough space to store thousands of high-resolution photographs. Video recorders, which once recorded video onto tapes or mini-CDs, now can save video footage in a digital format directly to a hard drive in the camera. The video files can be easily transferred from the video recorder to a computer. Many electronic storage devices (e.g., computers, cellular telephones, and tablets), have cameras built into the device which allows users to create and store still and video images on the device. Moreover, if the device has internet connectivity, users can distribute still and video images from the device.

c. Internet-enabled electronic storage devices can connect to other internet-enabled devices the world over. The ability to produce child pornography easily, reproduce it inexpensively, and market it anonymously (through electronic communications) has drastically changed the method of distribution and receipt of child pornography. Child pornography can be transferred via electronic mail or through file transfer protocols (FTP's) to anyone with access to an internet-enabled electronic storage device. Because of the proliferation of commercial services that provide electronic mail service, chat services (i.e., "Instant Messaging"), and easy access to the Internet, electronic storage devices are the preferred method of distribution and receipt of child pornographic materials.

d. Electronic storage devices are the ideal repository for child pornography. The amount of information that an electronic storage device can hold has grown exponentially over the last decade. Electronic storage devices can store thousands of images at very high resolution. In addition, there are numerous options available for the storage of computer or digital

files. One-terabyte external and internal hard drives are not uncommon. Other media storage devices include CDs, DVDs, and “thumb,” “jump,” or “flash” drives, which are very small devices that are plugged into a port on a computer or other electronic storage device. It is extremely easy for an individual to take a photo with a digital camera, upload that photo to a computer, and then copy it (or any other files on the computer) to any one of those media storage devices (CDs and DVDs are unique in that special software must be used to save or “burn” files onto them). Many electronic storage devices can easily be concealed and carried on an individual's person.

e. The Internet affords individuals several different venues for obtaining, viewing, and trading child pornography in a relatively secure and anonymous fashion.

f. Individuals also use online resources to retrieve and store child pornography, including services offered by Internet Portals such as Yahoo! and Google, among others. The online services allow a user to set up an account with a remote computing service that provides e-mail services as well as electronic storage of computer files in any variety of formats. A user can set up an online storage account from any internet-enabled electronic storage device. Even in cases where online storage is used, however, evidence of child pornography can be found on the user's electronic storage device in most cases.

g. As is the case with most digital technology, communications by way of electronic storage device can be saved or stored on the device. Storing this information can be intentional, i.e., by saving an e-mail as a file on the computer or saving the location of one's favorite websites in, for example, “bookmarked” files. Digital information can also be retained unintentionally, e.g., traces of the path of an electronic communication may be automatically

stored in many places (e.g., temporary files or ISP client software, among others). In addition to electronic communications, an electronic storage device user's Internet activities generally leave traces or "footprints" in the web cache and history files of the browser used. Such information is often maintained indefinitely until overwritten by other data.

h. Based on my knowledge, training, and experience, I know that electronic files or remnants of such files can be recovered months or even years after they have been downloaded onto a storage medium, deleted, or viewed via the Internet. Electronic files downloaded to a storage medium can be stored for years at little or no cost. Even when files have been deleted, they can be recovered months or years later using forensic tools. This is so because when a person "deletes" a file on a device, the data contained in the file does not actually disappear; rather, that data remains on the storage medium until it is overwritten by new data.

47. Based upon my training and experience and information relayed to me by agents and others involved in the forensic examination of computers, I know that computer data can be stored on a variety of systems and storage devices, including external and internal hard drives, flash drives, thumb drives, micro SD cards, macro SD cards, DVDs, gaming systems, SIM cards, cellular phones capable of storage, floppy disks, compact disks, magnetic tapes, memory cards, memory chips, and online or offsite storage servers maintained by corporations, including but not limited to "cloud" storage.

48. Additionally, based upon my training and experience and information related to me by agents and others involved in the forensic examination of computers, I know that routers, modems, and network equipment used to connect computers to the Internet often provide valuable evidence of, and are instrumentalities of, a crime. This is equally true of so-called "wireless

routers," which create localized networks that allow individuals to connect to the Internet wirelessly. Though wireless networks may be "secured" (in that they require an individual to enter an alphanumeric key or password before gaining access to the network) or "unsecured" (in that an individual may access the wireless network without a key or password), wireless routers for both secured and unsecured wireless networks may yield significant evidence of, or serve as instrumentalities of, a crime—including, for example, serving as the instrument through which the perpetrator of the Internet-based crime connected to the Internet and, potentially, containing logging information regarding the time and date of a perpetrator's network activity as well as identifying information for the specific device(s) the perpetrator used to access the network. Moreover, I know that individuals who have set up either a secured or unsecured wireless network in their residence are often among the primary users of that wireless network.

49. Based on my previous investigative experience related to child exploitation investigations, and the training and experience of other law enforcement officers with whom I have had discussions, I know there are certain characteristics common to individuals who transport, distribute, receive, possess, and/or access with intent to view child pornography:

a. Such individuals may receive sexual gratification, stimulation, and satisfaction from contact with children, or from fantasies they may have viewing children engaged in sexual activity or in sexually suggestive poses, such as in person, in photographs, or other visual media, or from literature describing such activity.

b. Such individuals may collect sexually explicit or suggestive materials in a variety of media, including photographs, magazines, motion pictures, videotapes, books, slides and/or drawings or other visual media. Individuals who have a sexual interest in children or images

of children oftentimes use these materials for their own sexual arousal and gratification. Further, they may use these materials to lower the inhibitions of children they are attempting to seduce, to arouse the selected child partner, or to demonstrate the desired sexual acts.

c. Likewise, such individuals often maintain their child pornography images in a digital or electronic format in a safe, secure, and private environment, such as a computer and surrounding area. These child pornography images are often maintained for several years and are kept close by, usually at the possessor's residence, inside the possessor's vehicle, or, at times, on their person, to enable the individual to view the child pornography images, which are valued highly. Some of these individuals also have been found to download, view, and then delete child pornography on their computers or digital devices on a cyclical and repetitive basis.

d. Importantly, evidence of such activity, including deleted child pornography, often can be located on these individuals' computers and digital devices using forensic tools. Indeed, the very nature of electronic storage means that evidence of the crime is often still discoverable for extended periods of time even after the individual "deleted" it.

e. Such individuals also may correspond with and/or meet others to share information and materials, rarely destroy correspondence from other child pornography distributors/possessors, conceal such correspondence as they do their sexually explicit material, and often maintain lists of names, addresses, and telephone numbers of individuals with whom they have been in contact and who share the same interests in child pornography.

f. Such individuals prefer not to be without their child pornography for any prolonged period. This behavior has been documented by law enforcement officers involved in the investigation of child pornography throughout the world. Thus, even if an individual, uses a

portable device (such as a mobile phone) to access the internet and child pornography, it is more likely than not that evidence of this access will be found in the SUBJECT PREMISES, as set forth in Attachment A.

### **CONCLUSION**

46. I respectfully request that this Court issue a search warrant for the location, and search of person described in Attachment A authorizing the seizure and search of the items described in Attachment B.

### **Attachment A**

#### DESCRIPTION OF LOCATIONS TO BE SEARCHED:

The entire property located at **N72W17809 GOOD HOPE RD, MENOMONEE FALLS, WI**. The location is more particularly described as a one-story single-family residence. This warrant authorizes the search of the SUBJECT PREMISES, any common areas accessible by the occupants of the SUBJECT PREMISES, any storage units or outbuildings associated with the SUBJECT PREMISES, as well as any appurtenances thereto. This warrant further authorizes the search of the following vehicles if located on the SUBJECT PREMISES: 2008 Ford F-350 (WI – XD86426), 2013 Jeep Wrangler (WI – ALY5708), 2007 Jeep Patriot (WI – ADT8690). The exterior of the SUBJECT PREMISES is tan stone siding. A white front door is located on the north side of the building facing Good Hope Road. A chimney is located on the north side of the building to the east of the front door as well as a white-trimmed window to the west of the front door.

Pictures of the residence are provided below:





- Computers and storage media found therein.
- Any person who appears to reside at the SUBJECT PREMISES.

## **Attachment B**

### **Items to be Seized**

1. Cell phones, computer(s), computer hardware, computer software, computer related documentation, computer passwords and data security devices, videotapes, video recording devices, video recording players, and video display monitors that may be, or are used to: visually depict child pornography or child erotica; display or access information pertaining to a sexual interest in child pornography; display or access information pertaining to sexual activity with children; or distribute, possess, or receive child pornography, child erotica, or information pertaining to an interest in child pornography or child erotica.
2. Any and all computer software, including programs to run operating systems, applications (such as word processing, graphics, or spreadsheet programs), utilities, compilers, interpreters, and communications programs.
3. Any and all notes, documents, records, or correspondence, in any format and medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes) pertaining to the possession, receipt, or distribution of child pornography as defined in 18 U.S.C. § 2256(8) or to the possession, receipt, or distribution of visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).
4. In any format and medium, all originals, computer files, copies, and negatives of child pornography as defined in 18 U.S.C. § 2256(8), visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2), or child erotica.
5. Any and all diaries, address books, names, and lists of names and addresses of individuals who may have been contacted by the operator of any device by use of the computer or by other

means for the purpose of distributing or receiving child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct as defined in 18 U.S.C. § 2256(2).

6. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and handwritten notes), identifying persons transmitting, through interstate or foreign commerce by any means, including, but not limited to, by the United States Mail or by computer, any child pornography as defined in 18 U.S.C. § 2256(8) or any visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).
7. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, other digital data files and web cache information) concerning the receipt, transmission, or possession of child pornography as defined in 18 U.S.C. § 2256(8) or visual depictions of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).
8. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) concerning communications between individuals about child pornography or the existence of sites on the Internet that contain child pornography or that cater to those with an interest in child pornography.
9. Any and all notes, documents, records, or correspondence, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic

messages, and other digital data files) concerning membership in online groups, clubs, or services that provide or make accessible child pornography to members.

10. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern any accounts with an Internet Service Provider.
11. Any and all records, documents, invoices and materials, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files) that concern online storage or other remote computer storage, including, but not limited to, software used to access such online storage or remote computer storage, user logs or archived data that show connection to such online storage or remote computer storage, and user logins and passwords for such online storage or remote computer storage.
12. Any and all cameras, film, videotapes or other photographic equipment.
13. Any and all visual depictions of minors.
14. Any and all address books, mailing lists, supplier lists, mailing address labels, and any and all documents and records, in any format or medium (including, but not limited to, envelopes, letters, papers, e-mail messages, chat logs and electronic messages, and other digital data files), pertaining to the preparation, purchase, and acquisition of names or lists of names to be used in connection with the purchase, sale, trade, or transmission, through interstate or foreign commerce by any means, including by the United States Mail or by computer, any child

pornography as defined in 18 U.S.C. § 2256(8) or any visual depiction of minors engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

15. Any and all diaries, notebooks, notes, and any other records reflecting personal contact and any other activities with minors visually depicted while engaged in sexually explicit conduct, as defined in 18 U.S.C. § 2256(2).

16. For any electronic storage device, computer hard drive, electronic device, or other physical object upon which electronic information can be recorded (hereinafter, “electronic storage device”) that is called for by this warrant, or that might contain things otherwise called for by this warrant:

- a. evidence of who used, owned, or controlled the electronic storage device at the time the things described in this warrant were created, edited, or deleted, such as logs, registry entries, configuration files, saved usernames and passwords, documents, browsing history, user profiles, email, email contacts, “chat,” instant messaging logs, photographs, and correspondence;
- b. evidence of software that would allow others to control the electronic storage device, such as viruses, Trojan horses, and other forms of malicious software, as well as evidence of the presence or absence of security software designed to detect malicious software;
- c. evidence of the lack of such malicious software;
- d. evidence indicating how and when the electronic storage device was accessed or used to determine the chronological context of electronic storage device access, use, and events relating to crime under investigation;

- e. evidence indicating the electronic storage device user's location and state of mind as it relates to the crime under investigation;
- f. evidence of the attachment to the electronic storage device of other storage devices or similar containers for electronic evidence;
- g. evidence of counter-forensic programs (and associated data) that are designed to eliminate data from the electronic storage device;
- h. evidence of the times the electronic storage device was used;
- i. passwords, encryption keys, and other access devices that may be necessary to access the electronic storage device;
- j. documentation and manuals that may be necessary to access the electronic storage device or to conduct a forensic examination of the electronic storage device;
- k. contextual information necessary to understand the evidence described in this attachment.

17. Records and things evidencing the use of the Internet Protocol addresses to communicate with the internet, including:

- a. routers, modems, and network equipment used to connect electronic storage devices to the Internet;
- b. records of Internet Protocol addresses used;
- c. records of Internet activity, including firewall logs, caches, browser history and cookies, "bookmarked" or "favorite" web pages, search terms that the user entered into any Internet search engine, and records of user-typed web addresses.

As used above, the terms "records" and "information" include all the foregoing items of evidence in whatever form and by whatever means they may have been created or stored, including

any form of electronic storage device or electronic storage; any handmade form (such as writing); any mechanical form (such as printing or typing); and any photographic form.

During the execution of the search of the premises described in Attachment A, law enforcement personnel are authorized to press the fingers (including thumbs) of residents of the SUBJECT PREMISES to the Touch ID sensor of device(s) or scan for facial recognition, such as an iPhone, Android, or Tablet, found at the premises for the purpose of attempting to unlock the device via fingerprint or facial recognition in order to search the contents as authorized by this warrant. If facial recognition is required, the subject will remain still and look, with eyes open, at the camera for any devices seized in connection if this warrant for the purpose of attempting to unlock the device(s) in order to search the contents as authorized by this warrant.